AMENDMENTS TO THE CLAIMS

Claim 1 (Currently Amended) An authentication system, comprising:

~~a portable recording medium~~ an IC card of ~~which~~ a forwarding agent ~~has~~;

an authentication apparatus operable to verify authenticity of a visit by the forwarding agent, the authentication apparatus being provided in a residence of a person ~~who is~~ visited by the forwarding agent; and

~~an input/output apparatus~~a card reader operable to perform inputting and outputting of information between the IC card ~~portable recording medium~~ and the authentication apparatus, the card reader ~~input/output apparatus~~ being for reading the IC card and being provided at an entrance of the residence~~, wherein~~

wherein the IC card ~~portable recording medium~~ stores~~, therein~~ in advance, at least one piece of information concerning the authenticity of the visit by the forwarding agent~~, and~~

wherein the authentication apparatus stores ~~therein~~ at least one piece of information ~~used~~ for verifying the authenticity of the visit by the forwarding agent, and judges whether or not the visit by the forwarding agent is authentic by, via the card reader ~~input/output apparatus~~, performing an authentication using (a) the information concerning the authenticity of the visit by the forwarding agent and stored in the IC card~~, portable recording medium~~ and (b) the information for verifying the authenticity of the visit by the forwarding agent and stored in the authentication apparatus,

wherein the IC card stores, as the information concerning the authenticity of the visit by the forwarding agent, certification information that certifies the authenticity of the visit by the forwarding agent, wherein the authentication apparatus stores, as the information for verifying the authenticity of the visit by the forwarding agent, authentication information used to examine the certification information,

wherein the card reader detects a lock status of an entrance door of the residence, such that, when the card reader detects that the entrance door is locked, the authentication apparatus performs, via the card reader, the authentication using the certification information from the IC card and the stored authentication information to judge whether or not the visit by the forwarding agent is authentic,

wherein the IC card further stores, as the information concerning the authenticity of the visit, first visit information that indicates a business of the visit by the forwarding agent,

wherein the authentication apparatus further stores, as the information for verifying the authenticity of the visit, second visit information used to examine the first visit information,

wherein, when a result of the authentication using the certification information from the IC card and the stored authentication information is positive, the authentication apparatus (c) acquires the first visit information from the IC card via the card reader, (d) judges whether or not the acquired first visit information matches the stored second visit information, and (e) when a result of the judgment of whether or not the acquired first visit information matches the stored second visit information is positive, judges that the visit by the forwarding agent is authentic,

wherein the authentication apparatus and the IC card perform a challenge-response authentication process using the certification information from the IC card and the stored authentication information,

wherein the authentication information is a secret key, wherein the IC card stores a first key that is obtained by executing a one-way function on a key that is identical to the secret key,

wherein the authentication apparatus generates challenge data, and outputs the generated challenge data to the IC card via the card reader,

wherein the IC card receives the challenge data from the authentication apparatus, generates encrypted response data by encrypting the challenge data using the first key, and outputs the encrypted response data to the authentication apparatus via the card reader, and

wherein the authentication apparatus receives the encrypted response data from the IC card, generates a second key by executing a function, which is identical to the one-way function, on the secret key, generates decrypted data by decrypting the encrypted response data using the generated second key, and performs the authentication by judging whether or not the generated decrypted data matches the challenge data.

Claims 2-4 (Cancelled)

Claim 5 (Currently Amended) The authentication system of Claim 1,~~ Claim 4, wherein~~

wherein the first visit information is first time information that indicates a first time period for the visit by the forwarding agent,

wherein the second visit information is second time information that indicates a second time period for the visit by the forwarding agent, and

wherein the authentication apparatus judges whether or not the first time information matches the second time information.

Claim 6 (Currently Amended) The authentication system of Claim 1, ~~Claim 4, wherein~~

wherein the first visit information is first business information that indicates a first business of the visit by the forwarding agent,

wherein the second visit information is second business information that indicates a second business of the visit by the forwarding agent, and

wherein the authentication apparatus judges whether or not the first business information matches the second business information.

Claim 7 (Currently Amended) The authentication system of Claim 1, ~~Claim 4, wherein~~

wherein the first visit information includes (i) first time information that indicates a first time period for the visit by the forwarding agent and (ii) first business information that indicates a first business of the visit by the forwarding agent,

wherein the second visit information includes (iii) second time information that indicates a second time period for the visit by the forwarding agent and (iv) second business information that indicates a second business of the visit by the forwarding agent, and

wherein the authentication apparatus judges whether or not the first time information matches the second time information, and judges whether or not the first business information matches the second business information.

Claim 8 (Currently Amended) The authentication system of Claim 1, ~~Claim 4, wherein~~

wherein the IC card further stores ~~therein~~ article information concerning an article delivered by the forwarding agent, and wherein the authentication apparatus further acquires the article information from the IC card via the card reader, and when ~~if~~ the authentication apparatus judges that the visit by the forwarding agent is authentic, displays the article information.

Claim 9 (Currently Amended) The authentication system of Claim 8, ~~wherein~~

wherein the article information is a name of a sender of the article, and

wherein the authentication apparatus acquires the name of the sender from the IC card and displays the acquired name.

Claim 10 (Currently Amended) The authentication system of Claim 8, ~~wherein~~

wherein the article information is a name of the article, and

wherein the authentication apparatus acquires the name of the article from the IC card and displays the acquired name of the article.

Claim 11 (Currently Amended) The authentication system of Claim 8, ~~wherein~~

wherein the article information is a message from a sender of the article, and

wherein the authentication apparatus acquires the message from the IC card and displays the acquired message.

Claim 12 (Currently Amended) The authentication system of Claim 1, ~~Claim 4, wherein~~

wherein the IC card further stores ~~therein~~ visitor information for identifying a visitor, and wherein the authentication apparatus further acquires the visitor information from the IC card via the card reader, and when ~~if~~ the authentication apparatus judges that the visit by the forwarding agent is authentic, displays the visitor information.

Claim 13 (Currently Amended) The authentication system of Claim 12,~~ wherein~~

wherein the visitor information is a name of the visitor, and

wherein the authentication apparatus acquires the name of the visitor from the IC card and displays the acquired name of the visitor.

Claim 14 (Currently Amended) The authentication system of Claim 12,~~ wherein~~

wherein the visitor information is an image of a facial photo of the visitor, and

wherein the authentication apparatus acquires the image of the facial photo of the visitor from the IC card and displays the acquired image of the facial photo.

Claim 15 (Currently Amended) The authentication system of Claim 12,~~ wherein~~

wherein the visitor information is a name and an image of a facial photo of the visitor, and

wherein the authentication apparatus acquires the name and the image of the facial photo of the visitor from the IC card and displays the acquired name and image of the facial photo.

Claims 16-29 (Cancelled)

Claim 30 (Currently Amended) The authentication system of Claim 1,~~ Claim 16, wherein~~

wherein the authentication apparatus further stores ~~therein~~ an apparatus identifier for identifying the authentication apparatus ~~itself~~,

wherein the authentication apparatus outputs the apparatus identifier to the IC card via the card reader when ~~if~~ the authentication apparatus judges that the visit by the forwarding agent is authentic, and

wherein the IC card, upon receiving the apparatus identifier from the authentication apparatus, stores ~~therein~~ the received apparatus identifier.

Claim 31 (Currently Amended) An authentication apparatus for verifying authenticity of a visit by a forwarding agent using a portable recording medium of ~~which~~ the forwarding agent ~~has~~, the authentication apparatus being provided in a residence of a person ~~who is~~ visited by the forwarding agent, the authentication apparatus comprising:

an information storage unit operable to store ~~therein~~ information ~~used~~ for ~~the~~ verifying ~~of~~ the authenticity of the visit by the forwarding agent; and

a judgment unit operable to judge whether or not the visit by the forwarding agent is authentic by, via a card reader for reading the portable recording medium of the forwarding agent and ~~an input/output apparatus~~ provided at an entrance of the residence, performing an authentication using information stored in the portable recording medium concerning the authenticity of the visit by the forwarding agent and using the stored information for verifying the authenticity of the visit by the forwarding agent ~~stored in the information storage unit~~,

wherein the card reader detects a lock status of an entrance door of the residence, wherein the portable recording medium stores, as the information concerning the authenticity of the visit by the forwarding agent, certification information that certifies the authenticity of the visit by the forwarding agent,

wherein the information storage unit stores, as the information for verifying the authenticity of the visit by the forwarding agent, authentication information used to examine the certification information,

wherein, when the card reader detects that the entrance door is locked, the judgment unit performs, via the card reader, the authentication by a challenge-response authentication process using the certification information from the portable recording medium and the stored authentication information to judge whether or not the visit by the forwarding agent is authentic,

wherein the portable recording medium further stores, as the information concerning the authenticity of the visit, first visit information that indicates a business of the visit by the forwarding agent,

wherein the information storage unit further stores, as the information for verifying the authenticity of the visit by the forwarding agent, second visit information used to examine the first visit information,

wherein, when a result of the authentication using the certification information from the portable recording medium and the stored authentication information is positive, the judgment unit (a) acquires the first visit information from the portable recording medium via the card reader, (b) judges whether or not the acquired first visit information matches the stored second visit information, and (c) when a result of the judgment of whether or not the acquired first visit information matches the stored second visit information is positive, judges that the visit by the forwarding agent is authentic, wherein the authentication information is a secret key,

wherein the portable recording medium stores a first key that is obtained by executing a one-way function on a key that is identical to the secret key,

wherein the judgment unit generates challenge data, and outputs the generated challenge data to the portable recording medium via the card reader, and

wherein, upon receiving encrypted response data, which is generated by encrypting the challenge data using the first key, from the portable recording medium via the card reader, the judgment unit (d) generates a second key by executing a function, which is identical to the one-way function, on the secret key, (e) generates decrypted data by decrypting the encrypted response data using the generated second key, and (f) performs the authentication by judging whether or not the generated decrypted data matches the challenge data.

Claims 32-34 (Cancelled)

Claim 35 (Currently Amended) The authentication apparatus of Claim 31, ~~Claim 34,~~ ~~wherein~~

wherein the portable recording medium further stores ~~therein~~ article information concerning an article delivered by the forwarding agent, and

wherein the authentication apparatus further comprises:

______an article information acquiring unit operable to acquire the article information from the portable recording medium via the card reader; and

______an article information display unit operable to display the article information when ~~if~~ the judgment unit judges that the visit by the forwarding agent is authentic.

Claim 36 (Currently Amended) The authentication apparatus of Claim 31, ~~Claim 34,~~ wherein

wherein the portable recording medium further stores ~~therein~~ visitor information for identifying a visitor, and

wherein the authentication apparatus further comprises:

a visitor information acquiring unit operable to acquire the visitor information from the portable recording medium via the card reader; and

a visitor information display unit operable to display the visitor information when ~~if~~ the judgment unit judges that the visit by the forwarding agent is authentic.

Claim 37 (Cancelled)

Claim 38 (Currently Amended) The authentication apparatus of Claim 31 ~~Claim 37~~, wherein the authentication apparatus is a mobile phone.

Claim 39 (Currently Amended) A portable recording medium of~~which~~ a forwarding agent ~~has~~ and ~~is~~ used by an authentication apparatus ~~operable~~ to verify authenticity of a visit by the forwarding agent, the authentication apparatus being provided in a residence of a person ~~who is~~ visited by the forwarding agent, the portable recording medium comprising:

a storage unit operable to store ~~therein~~, in advance, at least one piece of information concerning the authenticity of the visit by the forwarding agent;

a receiving unit operable to receive first data from the authentication apparatus via a card reader ~~an input/output apparatus~~ provided at an entrance of the residence;

a data generating unit operable to generate second data from the first data using the information concerning the authenticity of the visit by the forwarding agent and stored in the storage unit, the second data being used for an authentication process; and

an output unit operable to output the second data to the authentication apparatus via the card reader ~~input/output apparatus~~,

wherein the storage unit stores, as the information concerning the authenticity of the visit by the forwarding agent, certification information that certifies the authenticity of the visit of the forwarding agent,

wherein the data generating unit generates the second data using the certification information,

wherein the storage unit further stores, as the information concerning the authenticity of the visit by the forwarding agent, visit information that indicates a business of the visit by the forwarding agent,

wherein the output unit further outputs the visit information to the authentication apparatus via the card reader,

wherein the authentication apparatus stores authentication information used to examine the certification information,

wherein the authentication apparatus and the portable recording medium perform a challenge-response authentication process using the certification information from the portable recording medium and the stored authentication information,

wherein the authentication information is a secret key,

wherein the storage unit stores a first key that is obtained by executing a one-way function on a key that is identical to the secret key, wherein the authentication apparatus generates challenge data, and outputs the generated challenge data to the portable recording medium via the card reader,

wherein the data generating unit receives the challenge data from the authentication apparatus, and generates encrypted response data by encrypting the received challenge data using the first key,

wherein the output unit outputs the encrypted response data to the authentication apparatus via the card reader, and

wherein, upon receiving the encrypted response data from the portable recording medium, the authentication apparatus (a) generates a second key by executing a function, which is identical to the one-way function, on the secret key, (b) generates decrypted data by decrypting the encrypted response data using the generated second key, and (c) performs the authentication by judging whether or not the generated decrypted data matches the challenge data.

Claim 40 (Cancelled)

Claim 41 (Cancelled)

Claim 42 (Currently Amended) The portable recording medium of Claim 39 ~~Claim 41~~ further comprising an article information storage unit operable to store ~~therein~~ article information concerning an article delivered by the forwarding agent, ~~wherein~~

wherein the output unit further outputs the article information to the authentication apparatus via the card reader ~~input/output apparatus~~.

Claim 43 (Currently Amended) The portable recording medium of Claim 39 ~~Claim 41~~ further comprising a visitor information storage unit operable to store ~~therein~~ visitor information for identifying a visitor, ~~wherein~~

wherein the output unit further outputs the visitor information to the authentication apparatus via the card reader ~~input/output apparatus~~.

Claim 44 (Cancelled)

Claim 45 (Currently Amended) The portable recording medium of Claim 39 ~~Claim 44~~, wherein the portable recording medium is attached to a mobile phone.

Claim 46 (Currently Amended) An authentication method performed by ~~for~~ an authentication apparatus for verifying authenticity of a visit by a forwarding agent by using a portable recording medium of ~~which~~ the forwarding agent ~~has~~, the authentication apparatus being provided in a residence of a person ~~who is~~ visited by the forwarding agent,

wherein the authentication apparatus comprises ~~comprising:~~an information storage unit operable to store ~~therein~~ information ~~used~~ for ~~the~~ verifying ~~of~~ the authenticity of the visit by the forwarding agent, ~~and~~

wherein the authentication method comprises ~~comprising the step of~~:

a step of judging whether or not the visit by the forwarding agent is authentic by, via a card reader for reading the portable recording medium of the forwarding agent and ~~an input/output apparatus~~ provided at an entrance of the residence, performing an authentication using information stored in the portable recording medium concerning the authenticity of the visit by the forwarding agent and ~~using~~ the stored information for verifying the authenticity of the visit by the forwarding agent ~~stored in the information storage unit~~,

wherein the card reader detects a lock status of an entrance door of the residence,

wherein the portable recording medium stores, as the information concerning the authenticity of the visit by the forwarding agent, certification information that certifies the authenticity of the visit by the forwarding agent,

wherein the information storage unit stores, as the information for verifying the authenticity of the visit by the forwarding agent, authentication information used to examine the certification information,

wherein, when the card reader detects that the entrance door is locked, the step of judging performs, via the card reader, the authentication by a challenge-response authentication process using the certification information from the portable recording medium and the stored authentication information to judge whether or not the visit by the forwarding agent is authentic,

wherein the portable recording medium further stores, as the information concerning the authenticity of the visit by the forwarding agent, first visit information that indicates a business of the visit by the forwarding agent,

wherein the information storage unit further stores, as the information for verifying authenticity of the visit by the forwarding agent, second visit information used to examine the first visit information,

wherein, when a result of the authentication using the certification information from the portable recording medium and the stored authentication information is positive, the step of judging (a) acquires the first visit information from the portable recording medium via the card reader, (b) judges whether or not the acquired first visit information matches the stored second visit information, and (c) when a result of the judgment of whether or not the acquired first visit information matches the stored second visit information is positive, judges that the visit by the forwarding agent is authentic,

wherein the authentication information is a secret key,

wherein the portable recording medium stores a first key that is obtained by executing a one-way function on a key that is identical to the secret key,

wherein the step of judging generates challenge data, and outputs the generated challenge data to the portable recording medium via the card reader, and

wherein, upon receiving encrypted response data, which is generated by encrypting the challenge data using the first key, from the portable recording medium via the card reader, the judgment unit (d) generates a second key by executing a function, which is identical to the one-way function, on the secret key, (e) generates decrypted data by decrypting the encrypted response data using the generated second key, and (f) performs the authentication by judging whether or not the generated decrypted data matches the challenge data.

Claim 47 (Currently Amended) A non-transitory computer-readable recording medium having an authentication program recorded thereon, the~~An~~ authentication program being ran ~~that is run~~ in an authentication apparatus for verifying authenticity of a visit by a forwarding agent using a portable recording medium ~~which~~ of the forwarding agent ~~has~~, the authentication apparatus being provided in a residence of a person ~~who is~~ visited by the forwarding agent,

wherein the authentication apparatus comprises ~~comprising:~~ an information storage unit operable to store ~~therein~~ information ~~used~~ for ~~the~~ verifying ~~of~~ the authenticity of the visit by the forwarding agent, ~~and~~

wherein the authentication program causes a computer to execute a method comprising ~~comprising the step of~~:

a step of judging whether or not the visit by the forwarding agent is authentic by, via a card reader for reading the portable recording medium of the forwarding agent and ~~an input/output apparatus~~ provided at an entrance of the residence, performing an authentication using information stored in the portable recording medium concerning the authenticity of the visit by the forwarding agent and using the stored information for verifying the authenticity of the visit by the forwarding agent ~~stored in the information storage unit~~,

wherein the card reader detects a lock status of an entrance door of the residence,

wherein the portable recording medium stores, as the information concerning the authenticity of the visit by the forwarding agent, certification information that certifies the authenticity of the visit by the forwarding agent,

wherein the information storage unit stores, as the information for verifying the authenticity of the visit by the forwarding agent, authentication information used to examine the certification information,

wherein, when the card reader detects that the entrance door is locked, the step of judging performs, via the card reader, the authentication by a challenge-response authentication process using the certification information from the portable recording medium and the stored authentication information to judge whether or not the visit by the forwarding agent is authentic,

wherein the portable recording medium further stores, as the information concerning the authenticity of the visit by the forwarding agent, first visit information that indicates a business of the visit by the forwarding agent, wherein the information storage unit further stores, as the information for verifying authenticity of the visit by the forwarding agent, second visit information used to examine the first visit information,

wherein, when a result of the authentication using the certification information from the portable recording medium and the stored authentication information is positive, the step of judging (a) acquires the first visit information from the portable recording medium via the card reader, (b) judges whether or not the acquired first visit information matches the stored second visit information, and (c) when a result of the judgment of whether or not the acquired first visit information matches the stored second visit information is positive, judges that the visit by the forwarding agent is authentic,

wherein the authentication information is a secret key,

wherein the portable recording medium stores a first key that is obtained by executing a one-way function on a key that is identical to the secret key,

wherein the step of judging generates challenge data, and outputs the generated challenge data to the portable recording medium via the card reader, and

wherein, upon receiving encrypted response data, which is generated by encrypting the challenge data using the first key, from the portable recording medium via the card reader, the judgment unit (d) generates a second key by executing a function, which is identical to the one-way function, on the secret key, (e) generates decrypted data by decrypting the encrypted response data using the generated second key, and (f) performs the authentication by judging whether or not the generated decrypted data matches the challenge data.

Claim 48 (Cancelled)